TI - Exchange of cryptographic codes between terminal and network server - using exponential key exchange and random numbers to calculate and assure actuality of session key word at both sides without transmitting session key word between stations

PR - DE19951018546 19950519;DE19951018544 19950519;DE19951018545 19950519

PN - CN1186579 A 19980701 DW200266 H04L9/08 000pp
- DE19518546 C1 19960801 DW199635 H04L9/00 009pp
- WO9637064 A1 19961121 DW199701 H04L9/08 Ger 061pp
- EP0872076 A1 19981021 DW199846 H04L9/08 Ger 000pp
- JP11505384T T 19990518 DW199930 H04L9/08 052pp

PA - (SIEI) SIEMENS AG

IC - G06F12/14 ;G09C1/00 ;H04L9/00 ;H04L9/08

IN - HORN G; KESSLER V; MUELLER K

AB - DE19518546 The method comprises the steps of forming a first value (gt) in a user terminal (U) based on a random number, and transmitting that value in a first message (M1) to a network server. A session key word (K) is formed in the server based on a hash function (h1) on the exponential value formed on the first value and a secret network key (s). The server sends an answer (A) in a second message (M2) to the user terminal. A session key word (K) is formed in the user terminal, based on a hash function on an exponential value formed on a public network key (gs) and the first random number.
- The formed session key word is checked against the answer (A) of the server, and is input to a second hash function (h2) which supplies an input to a signature forming function (SigU). The resulting signature term and a identity value (IMUI) of the user terminal is transmitted to the server in a third message (M3), and validated to enable a session.
- USE/ADVANTAGE - Data security, e.g. in mobile telecommunications, chip-cards. Reduces length of necessary messages while improving security of codes.
- (Dwg.1/2)

OPD - 1995-05-19

CT - 3.Jnl.Ref;EP0307627;EP0460538

DN - CN JP US

DS - AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE LI

AN - 1996-342963 [02]

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 195 18 546 C 1**

(51) Int. Cl.[6]:
H 04 L 9/00
G 06 F 12/14

(21) Aktenzeichen: 195 18 546.3-31
(22) Anmeldetag: 19. 5. 95
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 1. 8. 96

DE 195 18 546 C 1

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Horn, Günther, Dr., 81541 München, DE; Kessler, Volker, Dr., 85256 Vierkirchen, DE; Müller, Klaus, 81539 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 52 22 140
US 51 53 919
US-Z.: BELLER, M. et al.: Privacy and Authentication on a Portable Communications System. In: IEEE Journal on Selected Areas in Communications, Vol.11, No.6, August 1993, S.821-829;
US-Z.: AZIS, A., DIFFIE, W.: Privacy and Authentication for Wireless Local Area Networks. In: IEEE Personal Communications, 1994, S. 25-31;
US-Z.: BELLER, M.: Proposed Authentication and Key Agreement Protocol for Personal Communications, P&A JEM 1993, S. 1-11;

(54) Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit U und einer Netzcomputereinheit N

(57) Die Erfindung betrifft ein Verfahren, mit dem ein Sitzungsschlüssel (K) zwischen einer Benutzercomputereinheit (U) und einer Netzcomputereinheit (N) vereinbart werden kann, ohne daß ein unbefugter Dritter nützliche Information bezüglich der Schlüssel oder der Identität der Benutzercomputereinheit (U) erhalten kann. Dies wird erreicht durch die Einbettung des Prinzips des El-Gamal Schlüsselaustauschs in das erfindungsgemäße Verfahren. Durch die Verwendung zweier Zufallszahlen (t, r) wird die Aktualität des Sitzungsschlüssels (K) gewährleistet. Der Sitzungsschlüssel (K) selbst wird niemals übertragen und kann somit nicht von einem unbefugten Dritten ermittelt werden.
Außerdem bietet das erfindungsgemäße Verfahren zusätzliche Sicherheitsmechanismen, wie z. B. die explizite Authentifikation der Netzcomputereinheit (N) durch die Benutzercomputereinheit (U) oder auch die Bestätigung des Sitzungsschlüssels (K) von der Netzcomputereinheit (N) an die Benutzercomputereinheit (B).

DE 195 18 546 C 1

Beschreibung

Informationstechnische Systeme unterliegen verschiedenen Bedrohungen. So kann z. B. übertragene Information von einem unbefugten Dritten abgehört und verändert werden. Eine weitere Bedrohung bei der Kommunikation zweier Kommunikationspartner liegt in der Vorspiegelung einer falschen Identität eines Kommunikationspartners.

Diesen und weiteren Bedrohungen wird durch verschiedene Sicherheitsmechanismen, die das informationstechnische System vor den Bedrohungen schützen sollen, begegnet. Ein zur Sicherung verwendeter Sicherheitsmechanismus ist die Verschlüsselung der übertragenen Daten. Damit die Daten in einer Kommunikationsbeziehung zwischen zwei Kommunikationspartnern verschlüsselt werden können, müssen vor der Übertragung der eigentlichen Daten erst Schritte durchgeführt werden, die die Verschlüsselung vorbereiten. Die Schritte können z. B. darin bestehen, daß sich die beiden Kommunikationspartner auf einen Verschlüsselungsalgorithmus einigen und daß ggf. die gemeinsamen geheimen Schlüssel vereinbart werden.

Besondere Bedeutung gewinnt der Sicherheitsmechanismus Verschlüsselung bei Mobilfunksystemen, da die übertragenen Daten in diesen Systemen von jedem Dritten ohne besonderen zusätzlichen Aufwand abgehört werden können.

Dies führt zu der Anforderung, eine Auswahl bekannter Sicherheitsmechanismen so zu treffen und diese Sicherheitsmechanismen geeignet zu kombinieren, sowie Kommunikationsprotokolle zu spezifizieren, daß durch sie die Sicherheit von informationstechnischen Systemen gewährleistet wird.

Es sind verschiedene asymmetrische Verfahren zum rechnergestützen Austausch kryptographischer Schlüssel bekannt. Asymmetrische Verfahren, die geeignet sind für Mobilfunksysteme, sind (A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Liocal Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) und (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11).

Das in (A. Aziz, W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, S. 25 bis 31) beschriebene Verfahren bezieht sich ausdrücklich auf lokale Netzwerke und stellt höhere Rechenleistungsanforderungen an die Computereinheiten der Kommunikationspartner während des Schlüsselaustauschs. Außerdem wird in dem Verfahren mehr Übertragungskapazität benötigt als in dem erfindungsgemäßen Verfahren, da die Länge der Nachrichten größer ist als bei dem erfindungsgemäßen Verfahren.

Das in (M. Beller, "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, 1993, S. 1 bis 11) beschriebene Verfahren hat einige grundlegende Sicherheitsziele nicht realisiert. Die explizite Authentifikation des Netzes durch den Benutzer wird nicht erreicht. Außerdem wird ein vom Benutzer an das Netz übertragener Schlüssel vom Netz nicht an den Benutzer bestätigt. Auch eine Zusicherung der Frische (Aktualität) des Schlüssels für das Netz ist nicht vorgesehen. Ein weiterer Nachteil dieses Verfahrens besteht in der Beschränkung auf das Rabin-Verfahren bei der impliziten Authentifizierung des Schlüssels durch den Benutzer. Dies schränkt das Verfahren in einer flexibleren Anwendbarkeit ein. Außerdem ist kein Sicherheitsmechanismus vorgesehen, der die Nichtabstreitbarkeit von übertragenen Daten gewährleistet. Dies ist ein erheblicher Nachteil vor allem auch bei der Erstellung unanfechtbarer Gebührenabrechnungen für ein Mobilfunksystem. Auch die Beschränkung des Verfahrens auf den National Institute of Standards in Technology Signature Standard (NIST DSS) als verwendete Signaturfunktion schränkt das Verfahren in seiner allgemeinen Verwendbarkeit ein.

Aus der US-Patentschrift US 5 222 140 ist ein Verfahren bekannt, bei dem unter Verwendung sowohl eines öffentlichen als auch eines geheimen Schlüssels sowie unter Verwendung einer Zufallszahl ein Sitzungsschlüssel erzeugt wird. Dieser wird mit einem öffentlichen Schlüssel verknüpft.

Dieses Verfahren weist im Vergleich zu dem erfindungsgemäßen Verfahren weniger realisierte grundlegende Sicherheitsziele auf.

Weiterhin ist aus der Patentschrift US 5 153 919 ein Verfahren beschrieben, bei dem eine Benutzereinheit sich gegenüber einer Netzeinheit identifiziert. Anschließend findet unter Anwendung einer Hash-Funktion zwischen der Benutzereinheit und der Netzeinheit ein Authentifizierungsprozeß statt.

Weitere sichere Kommunikationsprotokolle, die aber wesentliche grundlegende Sicherheitsziele nicht realisieren, sind bekannt (M. Beller et al, Privacy and Authentication on a Portable Communication System, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 6, S. 821—829, 1993).

Das Problem der Erfindung liegt darin, ein Verfahren zum rechnergestützten Austausch kryptographischer Schlüssel anzugeben, das die oben genannten Nachteile vermeidet.

Dieses Problem wird durch das Verfahren gemäß Patentanspruch 1 gelöst.

Die durch das erfindungsgemäße Verfahren erreichten Vorteile liegen vor allem in einer erheblichen Reduktion der Länge der übertragenen Nachrichten und in der Realisierung weiterer Sicherheitsziele.

Durch das erfindungsgemäße Verfahren werden folgende Sicherheitsziele realisiert:

- Gegenseitige explizite Authentifizierung von dem Benutzer und dem Netz, d. h. die gegenseitige Verifizierung der behaupteten Identität,
- Schlüsselvereinbarung zwischen dem Benutzer und dem Netz mit gegenseitiger impliziter Authentifizierung, d. h. daß durch das Verfahren erreicht wird, daß nach Abschluß der Prozedur ein gemeinsamer geheimer Sitzungsschlüssel zur Verfügung steht, von dem jede Partei weiß, daß nur das authentische Gegenüber sich ebenfalls im Besitz des geheimen Sitzungsschlüssels befinden kann,
- Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für den Benutzer,
- gegenseitige Bestätigung des Sitzungsschlüssels von dem Benutzer und dem Netz, d. h. die Bestätigung, daß das Gegenüber tatsächlich im Besitz des vereinbarten geheimen Sitzungsschlüssels ist.

Durch die Weiterbildung gemäß Patentanspruch 2 wird das Sicherheitsziel der Zusicherung der Frische (Aktualität) des Sitzungsschlüssels für das Netz realisiert.

Die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 3 ermöglicht die Verwendung von temporären Benutzeridentitäten.

Durch die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 4 wird das Sicherheitsziel der Benutzeranonymität realisiert, d. h. die Vertraulichkeit der Identität des Benutzers gegenüber Dritten.

Durch die Weiterbildung des erfindungsgemäßen Verfahrens gemäß Patentanspruch 6 wird zusätzlich das Sicherheitsziel der Nichtabstreitbarkeit von Daten realisiert, die vom Benutzer an das Netz gesendet wurden.

Das erfindungsgemäße Verfahren ist außerdem sehr leicht an unterschiedliche Anforderungen anpaßbar, da es sich nicht auf bestimmte Algorithmen für Signaturbildung und Verschlüsselung beschränkt.

Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Die Zeichnungen stellen bevorzugte Ausführungsbeispiele der Erfindung dar, die im folgenden näher beschrieben werden.

Es zeigen

Fig. 1 ein Ablaufdiagramm, das das erfindungsgemäße Verfahren gemäß Patentanspruch 1 darstellt;

Fig. 2 ein Diagramm, das das erfindungsgemäße Verfahren mit zusätzlich realisierten Sicherheitszielen gemäß einiger abhängiger Patentansprüche beschreibt.

Anhand der **Fig.** 1 und 2 wird die Erfindung weiter erläutert.

In den **Fig.** 1 und 2 sind durch zwei Skizzen der Ablauf des erfindungsgemäßen Verfahrens dargestellt. Das erfindungsgemäße Verfahren betrifft den Austausch kryptographischer Schlüssel zwischen einer Benutzercomputereinheit U und einer Netzcomputereinheit N, wobei unter der Benutzercomputereinheit U eine Computereinheit eines Benutzers eines Mobilfunknetzes zu verstehen ist und unter einer Netzcomputereinheit N eine Computereinheit des Netzbetreibers eines Mobilfunksystems zu verstehen ist.

Die Erfindung beschränkt sich jedoch nicht auf ein Mobilfunksystem und somit auch nicht auf einen Benutzer eines Mobilfunksystems und das Netz, sondern kann in allen Bereichen angewendet werden, in denen ein kryptographischer Schlüsselaustausch zwischen zwei Kommunikationspartnern benötigt wird. Dies kann z. B. in einer Kommunikationsbeziehung zwischen zwei Rechnern, die Daten in verschlüsselter Form austauschen wollen, der Fall sein. Ohne Beschränkung der Allgemeingültigkeit wird im folgenden also ein erster Kommunikationspartner als Benutzercomputereinheit U und ein zweiter Kommunikationspartner als Netzcomputereinheit N bezeichnet.

Für das erfindungsgemäße Verfahren gemäß Anspruch 1 wird vorausgesetzt, daß in der Benutzercomputereinheit U ein vertrauenswürdiger öffentlicher Netzschlüssel g^s der Netzcomputereinheit N verfügbar ist und daß in der Netzcomputereinheit N ein vertrauenswürdiger öffentlicher Benutzerschlüssel öu der Benutzercomputereinheit U verfügbar ist, wobei g ein erzeugendes Element einer endlichen Gruppe ist.

In der Benutzercomputereinheit U wird eine erste Zufallszahl t generiert. Aus der ersten Zufallszahl t wird mit Hilfe des erzeugenden Elements g einer endlichen Gruppe in der Benutzercomputereinheit U ein erster Wert g^t gebildet.

Asymmetrische Verfahren beruhen im wesentlichen auf zwei Problemen der Komplexitätstheorie, dem Problem zusammengesetzte Zahlen effizient zu faktorisieren, und dem diskreten Logarithmusproblem (DLP). Das DLP besteht darin, daß in geeigneten Rechenstrukturen zwar Exponentiationen effizient durchgeführt werden können, daß jedoch für die Umkehrung dieser Operation, das Logarithmieren, keine effizienten Algorithmen bekannt sind.

Solche Rechenstrukturen sind z. B. unter den oben bezeichneten endlichen Gruppen zu verstehen. Diese sind z. B. die multiplikative Gruppe eines endlichen Körpers (z. B. Multiplizieren Modulo p, wobei p eine große Primzahl ist), oder auch sogenannte "elliptische Kurven". Elliptische Kurven sind vor allem deshalb interessant, weil sie bei gleichem Sicherheitsniveau wesentliche kürzere Sicherheitsparameter erlauben. Dies betrifft die Länge der öffentlichen Schlüssel, die Länge der Zertifikate, die Länge der bei der Sitzungsschlüsselvereinbarung auszutauschenden Nachrichten sowie die Länge von digitalen Signaturen, die jeweils im weiteren beschrieben werden. Der Grund dafür ist, daß die für elliptische Kurven bekannten Logarithmierverfahren wesentlich weniger effizient sind als die für endliche Körper.

Eine große Primzahl in diesem Zusammenhang bedeutet, daß die Größe der Primzahl so gewählt werden muß, daß die Logarithmierung so aufwendig ist, daß sie nicht in vertretbarer Zeit durchgeführt werden kann. Vertretbar bedeutet in diesem Zusammenhang einen Zeitraum entsprechend der Sicherheitspolitik von mehreren Jahren bis Jahrzehnten und länger.

Nach der Berechnung des ersten Werts g^t wird eine erste Nachricht M1 codiert, die mindestens den ersten Wert g^t aufweist. Die erste Nachricht M1 wird von der Benutzercomputereinheit U an die Netzcomputereinheit N übertragen.

In der Netzcomputereinheit N wird die erste Nachricht M1 decodiert. Die erste Nachricht M1 kann auch über einen unsicheren Kanal, also auch über eine Luftschnittstelle, unverschlüsselt übertragen werden, da die Logarithmierung des ersten Wertes g^t nicht in vertretbarer Zeit durchgeführt werden kann.

Wie in **Fig.** 2 beschrieben, kann es vorgesehen sein, daß in der Netzcomputereinheit N eine zweite Zufallszahl r generiert wird. Durch diesen zusätzlichen Verfahrensschritt wird ein zusätzliches Sicherheitsziel realisiert: die Zusicherung der Frische (Aktualität) eines im folgenden beschriebenen Sitzungsschlüssels K für die Netzcomputereinheit N.

In der Netzcomputereinheit N wird mit Hilfe einer ersten Hash-Funktion h1 ein Sitzungsschlüssel K gebildet. Als eine erste Eingangsgröße der ersten Hash-Funktion h1 wird mindestens ein erster Term verwendet. Der erste Term wird gebildet, indem der erste Wert g^t potenziert wird mit einem geheimen Netzschlüssels.

Unter einer Hash-Funktion ist in diesem Zusammenhang eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfolge fester Länge zugeordnet. Des weiteren wird für die Hash-Funktion in diesem Zusammenhang Kollisionsfreiheit gefordert, d. h. es darf nicht möglich sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben.

Wenn die zweite Zufallszahl r verwendet wird, so weist die erste Eingangsgröße der ersten Hash-Funktion h1 zusätzlich mindestens die zweite Zufallszahl r auf.

Nun wird in der Netzcomputereinheit N eine Ant-

wort A gebildet. Zur Bildung der Antwort A sind verschiedene Varianten vorgesehen. So ist es z. B. möglich, daß mit dem Sitzungsschlüssel K unter Verwendung einer Verschlüsselungsfunktion Enc eine Konstante const verschlüsselt wird. Die Konstante const ist sowohl der Benutzercomputereinheit U als auch der Netzcomputereinheit N bekannt. Auch die Verschlüsselungsfunktion Enc ist sowohl der Netzcomputereinheit N als auch der Benutzercomputereinheit U als die in dem erfindungsgemäßen Verfahren zu verwendende Verschlüsselungsfunktion bekannt.

Eine weitere Möglichkeit, die Antwort A zu bilden liegt z. B. darin, daß der Sitzungsschlüssel K als Eingangsgröße für eine dritte Hash-Funktion h3 verwendet wird und der "gehashte" Wert des Sitzungsschlüssels K als Antwort A verwendet wird. Weitere Möglichkeiten, die Antwort A zu bilden, die zur Überprüfung des Sitzungsschlüssels K in der Benutzercomputereinheit U verwendet wird, sind dem Fachmann geläufig und können als Varianten zu den beschriebenen Vorgehensweisen verwendet werden.

Eine Aneinanderreihung der zweiten Zufallszahl r, der Antwort A, sowie ein optionales erstes Datenfeld dat1 bilden eine zweite Nachricht M2. Die zweite Zufallszahl r und das optionale erste Datenfeld dat1 sind nur in der zweiten Nachricht 112 enthalten, wenn diese in dem erfindungsgemäßen Verfahren vorgesehen werden.

Die zweite Nachricht M2 wird in der Netzcomputereinheit N codiert und zu der Benutzercomputereinheit U übertragen.

In der Benutzercomputereinheit U wird die zweite Nachricht M2 decodiert, so daß die Benutzercomputereinheit U eventuell die zweite Zufallszahl r, die Antwort A sowie eventuell das optionale erste Datenfeld dat1 zur Verfügung hat. Die Länge des optionalen ersten Datenfeldes dat1 kann beliebig groß sein, d. h. es ist auch möglich, daß das optionale erste Datenfeld dat1 nicht vorhanden ist.

In der Benutzercomputereinheit U wird nun ebenfalls der Sitzungsschlüssel K gebildet, mit Hilfe der ersten Hash-Funktion h1, die sowohl der Netzcomputereinheit N als auch der Benutzercomputereinheit U bekannt ist. Eine zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der Benutzercomputereinheit U weist mindestens einen zweiten Term auf. Der zweite Term wird gebildet aus einer Exponentation eines öffentlichen Netzschlüssels g^s mit der ersten Zufallszahl t. Wenn die Verwendung der zweiten Zufallszahl r in dem erfindungsgemäßen Verfahren vorgesehen wird, so weist die zweite Eingangsgröße der ersten Hash-Funktion h1 zur Bildung des Sitzungsschlüssels K in der Benutzercomputereinheit U zusätzlich die zweite Zufallszahl auf.

Durch die Verwendung der ersten Zufallszahl t und der zweiten Zufallszahl r bei der Generierung des Sitzungsschlüssels K wird die Aktualität des Sitzungsschlüssels K gewährleistet, da jeweils die erste Zufallszahl t als auch die zweite Zufallszahl r nur für jeweils einen Sitzungsschlüssel K verwendet werden.

Somit wird eine Wiedereinspielung eines älteren Schlüssels als Sitzungsschlüssel K verhindert. Die Aktualität des Sitzungsschlüssels K ist auch bedeutend im Zusammenhang mit der Fragestellung, wie groß die erste Zufallszahl t sowie die zweite Zufallszahl r sein müssen. Dies wird deutlich, da eine geringere Länge der Zufallszahlen das DLP-Problem verringern, d. h. je kürzer die Zufallszahl ist, desto einfacher ist die Logarithmierung, also z. B. das Herausfinden der ersten Zufallszahl t aus dem ersten Wert g^t. Wenn aber für jeden neuen Sitzungsschlüssel K andere Zufallszahlen verwendet werden, so ist die Wahrscheinlichkeit, daß der verwendete Sitzungsschlüssel K von einem unbefugten Dritten schon herausgefunden wurde, wesentlich geringer. Damit ist die Gefahr, daß der Teil einer Nachricht, der mit dem Sitzungsschlüssel K verschlüsselt ist, von einem unbefugten Dritten entschlüsselt werden kann, erheblich reduziert.

Nachdem in der Benutzercomputereinheit U der Sitzungsschlüssel K gebildet wurde, wird anhand der empfangenen Antwort A überprüft, ob der in der Benutzercomputereinheit U gebildete Sitzungsschlüssel K mit dem Sitzungsschlüssel K, der in der Netzcomputereinheit N gebildet wurde, übereinstimmt. Abhängig von den im vorigen beschriebenen Varianten zur Bildung der Antwort A sind verschiedene Möglichkeiten vorgesehen, den Sitzungsschlüssel K anhand der Antwort A zu überprüfen.

Eine Möglichkeit besteht z. B. darin, daß, wenn die Antwort A in der Netzcomputereinheit N durch Verschlüsselung der Konstante const mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc gebildet wurde, die Antwort A entschlüsselt wird, und somit die Benutzercomputereinheit U eine entschlüsselte Konstante const' erhält, die mit der bekannten Konstante const verglichen wird.

Die Überprüfung des Sitzungsschlüssels K anhand der Antwort A kann auch durchgeführt werden, indem die der Benutzercomputereinheit U bekannte Konstante const mit dem in der Benutzercomputereinheit U gebildeten Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird und das Ergebnis mit der Antwort A auf Übereinstimmung geprüft wird. Diese Vorgehensweise wird z. B. auch verwendet, wenn die Antwort A in der Netzcomputereinheit N gebildet wird, indem auf den Sitzungsschlüssel K die dritte Hash-Funktion h3 angewendet wird. In diesem Fall wird in der Benutzercomputereinheit U der in der Benutzercomputereinheit U gebildete Sitzungsschlüssel K als Eingangsgröße der dritten Hash-Funktion h3 verwendet. Der "gehashte" Wert des in der Benutzercomputereinheit U gebildeten Sitzungsschlüssels K wird dann mit der Antwort A auf Übereinstimmung geprüft. Damit wird das Ziel der Schlüsselbestätigung des Sitzungsschlüssels K erreicht.

Dadurch, daß bei der Berechnung des Sitzungsschlüssels K in der Netzcomputereinheit N der geheime Netzschlüssel s und bei der Berechnung des Sitzungsschlüssels K in der Benutzercomputereinheit U der öffentliche Netzschlüssel g^s verwendet werden, wird die Netzcomputereinheit N durch die Benutzercomputereinheit U authentifiziert. Dies wird erreicht, vorausgesetzt daß für die Benutzercomputereinheit U bekannt ist, daß der öffentliche Netzschlüssel g^s tatsächlich zur Netzcomputereinheit N gehört.

Im Anschluß an die Bestätigung des Sitzungsschlüssels K durch Überprüfung der Antwort A wird ein Signaturterm berechnet. Hierzu wird mit Hilfe einer zweiten Hash-Funktion h2 eine vierte Eingangsgröße gebildet. Die zweite Hash-Funktion h2 kann, muß aber nicht dieselbe Hash-Funktion sein wie die erste Hash-Funktion h1. Als eine dritte Eingangsgröße für die zweite Hash-Funktion h2 wird ein Term verwendet, der mindestens den Sitzungsschlüssel K enthält. Weiterhin kann die dritte Eingangsgröße das optionale erste Datenfeld dat1 oder auch ein optionales zweites Datenfeld dat2

enthalten, wenn deren Verwendung in dem erfindungsgemäßen Verfahren vorgesehen wird.

Es kann später nicht abgestritten werden, daß die Daten, die im ersten optionale Datenfeld dat1 und im zweiten optionalen Datenfeld dat2 enthalten sind, von der Benutzercomputereinheit U gesendet wurden.

Die in dem ersten optionalen Datenfeld dat1 und in dem zweiten optionalen Datenfeld dat2 enthaltenen Daten können z. B. Telefonnummern, die aktuelle Zeit oder ähnliche hierfür geeignete Parameter sein. Diese Information kann als Werkzeug für eine unanfechtbare Gebührenabrechnung verwendet werden.

Unter Verwendung einer ersten Signaturfunktion Sig_U wird der Signaturterm aus mindestens der vierten Eingangsgröße gebildet. Um einen höheren Sicherheitsgrad zu erzielen, kann der Signaturterm verschlüsselt werden. Der Signaturterm wird in diesem Fall mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt und bildet den ersten verschlüsselten Term VT1.

Außerdem wird, falls das Sicherheitsziel "Anonymität des Benutzers" realisiert werden soll, ein zweiter verschlüsselter Term VT2 berechnet, in dem eine Identitätsgröße IMUI der Benutzercomputereinheit U mit dem Sitzungsschlüssel K mit Hilfe der Verschlüsselungsfunktion Enc verschlüsselt wird. Bei Verwendung eines optionalen zweiten Datenfeldes dat2 wird in der Benutzercomputereinheit U ein dritter verschlüsselter Term VT3 berechnet, indem das optionale zweite Datenfeld dat2 mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird, das optionale zweite Datenfeld dat2 kann auch unverschlüsselt übertragen werden.

In der Benutzercomputereinheit U wird eine dritte Nachricht M3 gebildet und codiert, die mindestens den Signaturterm und die Identitätsgröße |MU| der Benutzercomputereinheit U aufweist.

Falls die Anonymität der Benutzercomputereinheit U gewährleistet werden soll, weist die dritte Nachricht M3 anstatt der Identitätsgröße |MU| der Benutzercomputereinheit U mindestens den zweiten verschlüsselten Term VT2 auf, der die Information aber die Identität der Benutzercomputereinheit U in verschlüsselter Form enthält, die nur von der Netzcomputereinheit N entschlüsselt werden kann.

Wenn die Verwendung des optionalen zweiten Datenfelds dat2 vorgesehen wird, weist die dritte Nachricht M3 zusätzlich mindestens den dritten verschlüsselten Term VT3 oder das optionale zweite Datenfeld dat2 im Klartext auf.

Wenn die dritte Nachricht M3 den ersten verschlüsselten Term VT1, den zweiten verschlüsselten Term VT2 oder den dritten verschlüsselten Term VT3 enthält, werden diese in der Netzcomputereinheit N entschlüsselt. Dies geschieht für den eventuell vorhandenen ersten verschlüsselten Term VT1 vor der Verifikation des Signaturterms.

Die dritte Nachricht M3 wird von der Benutzercomputereinheit U zu der Netzcomputereinheit N übertragen.

Zusätzlich wird die Authentifikation der Benutzercomputereinheit U gegenüber der Netzcomputereinheit N durch den Signaturterm gewährleistet, durch deren Verwendung garantiert wird, daß die dritte Nachricht M3 tatsächlich aktuell von der Benutzercomputereinheit U gesendet wurde.

In der Netzcomputereinheit N wird die dritte Nachricht M3 decodiert und anschließend wird anhand eines Benuterzertifikats CertU, das der Netzcomputereinheit N zur Verfügung steht, der Signaturterm verifiziert.

Wenn für das erfindungsgemäße Verfahren temporäre Benutzeridentitäten vorgesehen werden, so wird das im vorigen beschriebene Verfahren um einige Verfahrensschritte erweitert.

Zuerst muß der Netzcomputereinheit N bekannt gemacht werden, welche Benutzercomputereinheit U eine neue temporäre Identitätsgröße TMUIN von der Netzcomputereinheit N zugewiesen bekommen soll.

Hierzu wird als zusätzlicher Bestandteil der ersten Nachricht M1 eine alte temporäre Identitätsgröße TMUIO von der Benutzercomputereinheit U an die Netzcomputereinheit N übertragen.

Nach Empfang der ersten Nachricht M1 ist somit in der Netzcomputereinheit N bekannt, für welche Benutzercomputereinheit U die neue temporäre Identitätsgröße TMUIN bestimmt ist.

In der Netzcomputereinheit N wird dann die neue temporäre Identitätsgröße TMUIN für die Benutzercomputereinheit U gebildet. Dies kann z. B. durch Generierung einer Zufallszahl oder durch Tabellen, in denen mögliche Identitätsgrößen abgespeichert sind, durchgeführt werden. Aus der neuen temporären Identitätsgröße TMUIN der Benutzercomputereinheit U wird in der Netzcomputereinheit N ein vierter verschlüsselter Term VT4 gebildet, indem die neue temporäre Identitätsgröße TMUIN der Benutzercomputereinheit U mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird.

In diesem Fall weist die zweite Nachricht N2 zusätzlich mindestens den vierten verschlüsselten Term VT4 auf. Der vierte verschlüsselte Term VT4 wird dann in der Benutzercomputereinheit U entschlüsselt. Nun ist die neue temporäre Identitätsgröße TMUIN der Benutzercomputereinheit U in der Benutzercomputereinheit U verfügbar.

Damit der Netzcomputereinheit N auch gewährleistet wird, daß die Benutzercomputereinheit U die neue temporäre Identitätsgröße TMUIN korrekt empfangen hat, weist die dritte Eingangsgröße für die erste Hash-Funktion h1 oder für die zweite Hash-Funktion h2 zusätzlich mindestens die neue temporäre Identitätsgröße TMUIN der Benutzercomputereinheit U auf.

Da die Information der neuen temporären Identitätsgröße TMUIN in dem Signaturterm in diesem Fall enthalten ist, weist die dritte Nachricht M3 nicht mehr die Identitätsgröße IMUI der Benutzercomputereinheit U auf.

Es ist auch möglich, die neue temporäre Identitätsgröße TMUIN nicht in den Signaturterm zu integrieren, sondern den zweiten verschlüsselten Term VT2 zu bilden, indem anstatt der Identitätsgröße |MU| der Benutzercomputereinheit U die neue temporäre Identitätsgröße TMUIN mit dem Sitzungsschlüssel K unter Verwendung der Verschlüsselungsfunktion Enc verschlüsselt wird. In diesem Fall weist die dritte Nachricht M3 zusätzlich den zweiten verschlüsselten Temr VT2 auf.

Die in dem erfindungsgemäßen Verfahren verwendeten Hash-Funktionen, die erste Hash-Funktion h1, die zweite Hash-Funktion h2 und die dritte Hash-Funktion h3 können durch die gleiche, aber auch durch verschiedene Hash-Funktionen realisiert werden.

Patentansprüche

1. Verfahren zum rechnergestützten Austausch

kryptographischer Schlüssel zwischen einer Benutzercomputereinheit (U) und einer Netzcomputereinheit (N),

— bei dem aus einer ersten Zufallszahl (t) mit Hilfe eines erzeugenden Elements (g) einer endlichen Gruppe in der Benutzercomputereinheit (U) ein erster Wert (g^t) gebildet wird,

— bei eine erste Nachricht (M1) von der Benutzercomputereinheit (U) an die Netzcomputereinheit (N) übertragen wird, wobei die ersten Nachricht (M1) mindestens den ersten Wert (g^t) aufweist,

— bei dem in der Netzcomputereinheit (N) ein Sitzungsschlüssel (K) mit Hilfe einer ersten Hash-Funktion (h1) gebildet wird, wobei eine erste Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen ersten Term aufweist, der gebildet wird durch eine Exponentiation des ersten Werts (g^t) mit einem geheimen Netzschlüssel (s),

— bei dem in der Netzcomputereinheit (N) eine Antwort (A) gebildet wird,

— bei dem eine zweite Nachricht (M2) von der Netzcomputereinheit (N) an die Benutzercoinputereinheit (U) übertragen wird, wobei die zweite Nachricht (M2) mindestens die Antwort (A) aufweist,

— bei dem in der Benutzercomputereinheit (U) der Sitzungsschlüssel (K) gebildet wird mit Hilfe der ersten Hash-Funktion (h1), wobei eine zweite Eingangsgröße der ersten Hash-Funktion (h1) mindestens einen zweiten Term aufweist, der gebildet wird durch eine Exponentiation eines öffentlichen Netzschlüssels (g^t) mit der ersten Zufallszahl (t),

— bei dem in der Benutzercomputereinheit (U) der Sitzungsschlüssel (K) anhand der Antwort (A) überprüft wird,

— bei dem in der Benutzercomputereinheit (U) mit Hilfe einer zweiten Hash-Funktion (h2) oder der ersten Hash-Funktion (h1) eine vierte Eingangsgröße gebildet wird, wobei eine dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße mindestens den Sitzungsschlüssel (K) aufweist,

— bei dem in der Benutzercomputereinheit (U) ein Signaturterm aus mindestens der vierten Eingangsgröße gebildet wird unter Anwendung einer ersten Signaturfunktion (Sigu),

— bei dem eine dritte Nachricht (M3) von der Benutzercomputereinheit (U) an die Netzcomputereinheit (N) übertragen wird, wobei die dritte Nachricht (M3) mindestens den Signaturterm und eine Identitätsgröße (IMUI) der Benutzercomputereinheit (U) aufweist, und

— bei dem in der Netzcomputereinheit (N) der Signaturterm verifiziert wird.

2. Verfahren nach Anspruch 1,

— bei dem in der Netzcomputereinheit (N) die erste Eingangsgröße der ersten Hash-Funktion (h1) zusätzlich mindestens eine zweite Zufallszahl (r) aufweist,

— bei dem die zweite Nachricht (M2) zusätzlich die zweite Zufallszahl (r) aufweist, und

— bei dem in der Benutzercomputereinheit (U) die zweite Eingangsgröße der ersten Hash-Funktion (h1) zusätzlich mindestens die zweite Zufallszahl (r) aufweist.

3. Verfahren nach Anspruch 1 oder 2,

— bei dem die erste Nachricht (M1) zusätzlich mindestens eine alte temporäre Identitätsgröße (TMUIO) der Benutzercomputereinheit (U) aufweist,

— bei dem in der Netzcomputereinheit (N), nach dem die ersten Nachricht (M1) empfangen wurde und bevor die zweite Nachricht (M2) gebildet wird, für die Benutzercomputereinheit (U) eine neue temporäre Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) gebildet wird,

— bei dem aus der neuen temporären Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) ein vierter verschlüsselter Term (VT4) gebildet wird, in dem die neue temporäre Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die zweite Nachricht (M2) zusätzlich mindestens den vierten verschlüsselten Term (VT4) aufweist,

— bei dem in der Benutzercomputereinheit (U), nachdem die zweite Nachricht (M2) empfangen wurde und bevor die vierte Eingangsgröße gebildet wird, der vierte verschlüsselte Term (VT4) entschlüsselt wird,

— bei dem die dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße zusätzlich mindestens die neue temporäre Identitätsgröße (TMUIN) der Benutzercomputereinheit (U) aufweist, und

— bei dem die dritte Nachricht (M3) nicht die Identitätsgröße (IMUI) der Benutzercomputereinheit (U) aufweist.

4. Verfahren nach einem der Anschlüsse 1 bis 3,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der dritten Nachricht (M3) aus der Identitätsgröße (IMUI) der Benutzercomputereinheit (U) ein zweiter verschlüsselter Term (VT2) gebildet wird, in dem die Identitätsgröße (IMUI) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die dritte Nachricht (M3) anstatt der Identitätsgröße (IMUI) der Benutzercomputereinheit (U) den zweiten verschlüsselten Term (VT2) aufweist, und

— bei dem in der Netzcomputereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde, der zweite verschlüsselte Term (VT2) entschlüsselt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4,

— bei dem die zweite Nachricht (M2) zusätzlich ein optionales erstes Datenfeld (dat1) aufweist und

— bei dem die dritte Eingangsgröße für die erste Hash-Funktion (h1) oder für die zweite Hash-Funktion (h2) zur Bildung der vierten Eingangsgröße zusätzlich mindestens das optionale erste Datenfeld (dat1) aufweist.

6. Verfahren nach einem der Ansprüche 1 bis 5,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der dritten Nachricht (M3) ein dritter verschlüsselter Term (VT3) gebildet

wird, indem ein optionales zweites Datenfeld (dat2) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die dritte Nachricht (M3) zusätzlich mindestens den dritten verschlüsselten Term (VT3) aufweist, und

— bei dem in der Netzcomputereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde, der dritte verschlüsselte Term (VT3) entschlüsselt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6,

— bei dem in der Benutzercomputereinheit (U) vor Bildung der dritten Nachricht (M3) ein erster verschlüsselter Term (VT1) gebildet wird, indem der Signaturterm mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird,

— bei dem die dritte Nachricht (M3) anstatt des Signaturterms den ersten verschlüsselten Term (VT1) aufweist, und

— bei dem in der Netzcomputereinheit (N), nachdem die dritte Nachricht (M3) empfangen wurde und bevor der Signaturterm verifiziert wird, der erste verschlüsselte Term (VT1) entschlüsselt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem in der Netzcomputereinheit (N) die Antwort (A) gebildet wird, indem eine Konstante (const), die in der Netzcomputereinheit (N) und in der Benutzercomputereinheit (U) bekannt sind, mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird.

9. Verfahren nach einem der Ansprüche 1 bis 7,

— bei dem in der Netzcomputereinheit (N) die Antwort (A) gebildet wird, indem auf den Sitzungsschlüssel (K) eine dritte Hash-Funktion (h3) angewendet wird, und

— bei dem in der Benutzercomputereinheit (U) die Antwort (A) überprüft wird, indem auf den Sitzungsschlüssel (K) die dritte Hash-Funktion (h3) angewendet wird, und das Ergebnis mit der Antwort (A) verglichen wird.

10. Verfahren nach einem der Ansprüche 1 bis 7 oder 9, bei dem in der Benutzercomputereinheit (U) die Antwort (A) überprüft wird, indem die Konstante (const) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) verschlüsselt wird und das Ergebnis mit der Antwort (A) verglichen wird.

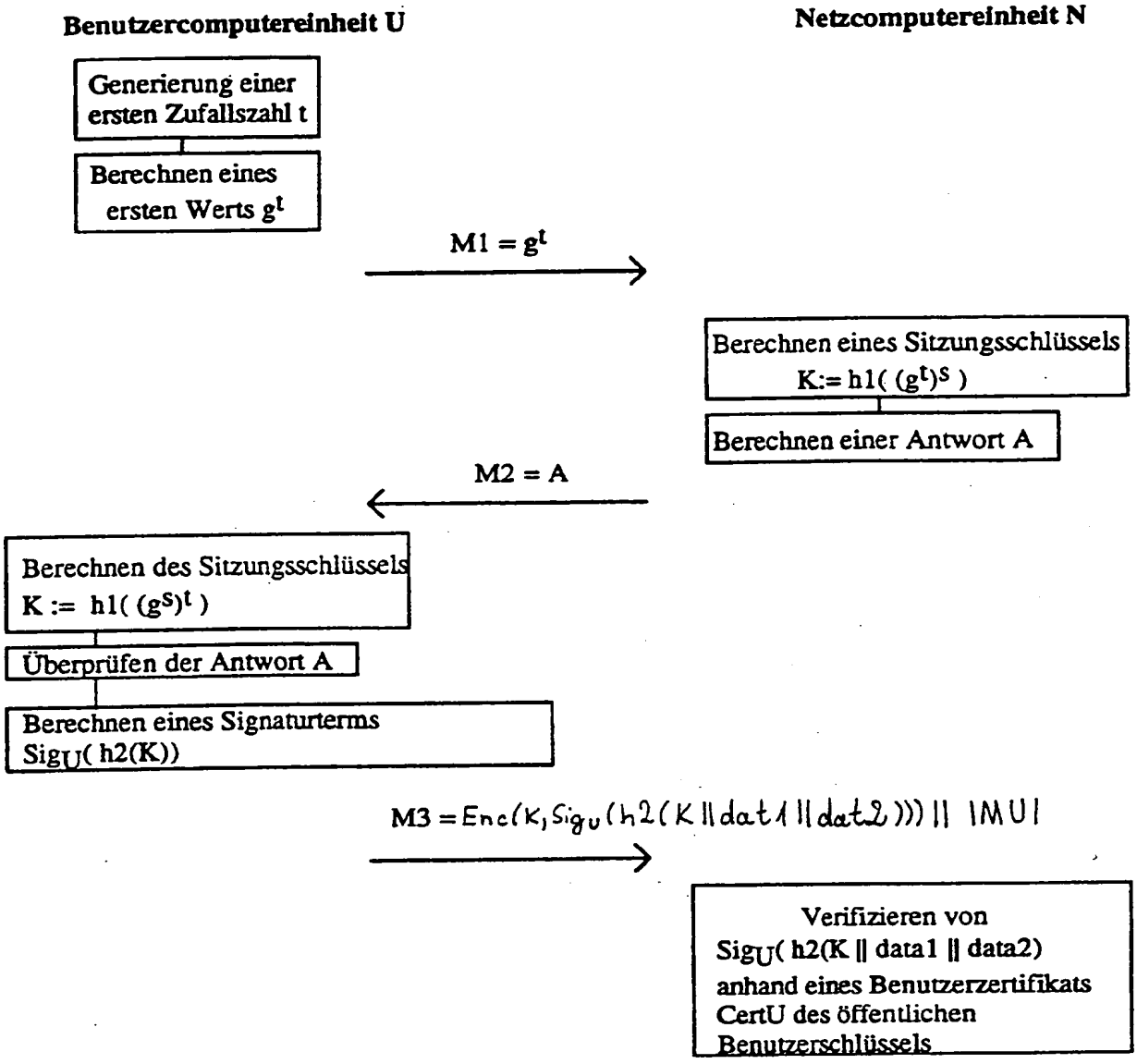
11. Verfahren nach einem der Ansprüche 1 bis 7 oder 9, bei dem in der Benutzercomputereinheit (U) die Antwort (A) überprüft wird, indem die Antwort (A) mit dem Sitzungsschlüssel (K) unter Anwendung der Verschlüsselungsfunktion (Enc) entschlüsselt wird und eine entschlüsselte Konstante (const') mit der Konstante (const) verglichen wird.

12. Verfahren nach einem der Ansprüche 1 bis 5, bei dem die dritte Nachricht (M3) zusätzlich mindestens ein optionales zweites Datenfeld (dat2) aufweist.

Hierzu 2 Seite(n) Zeichnungen

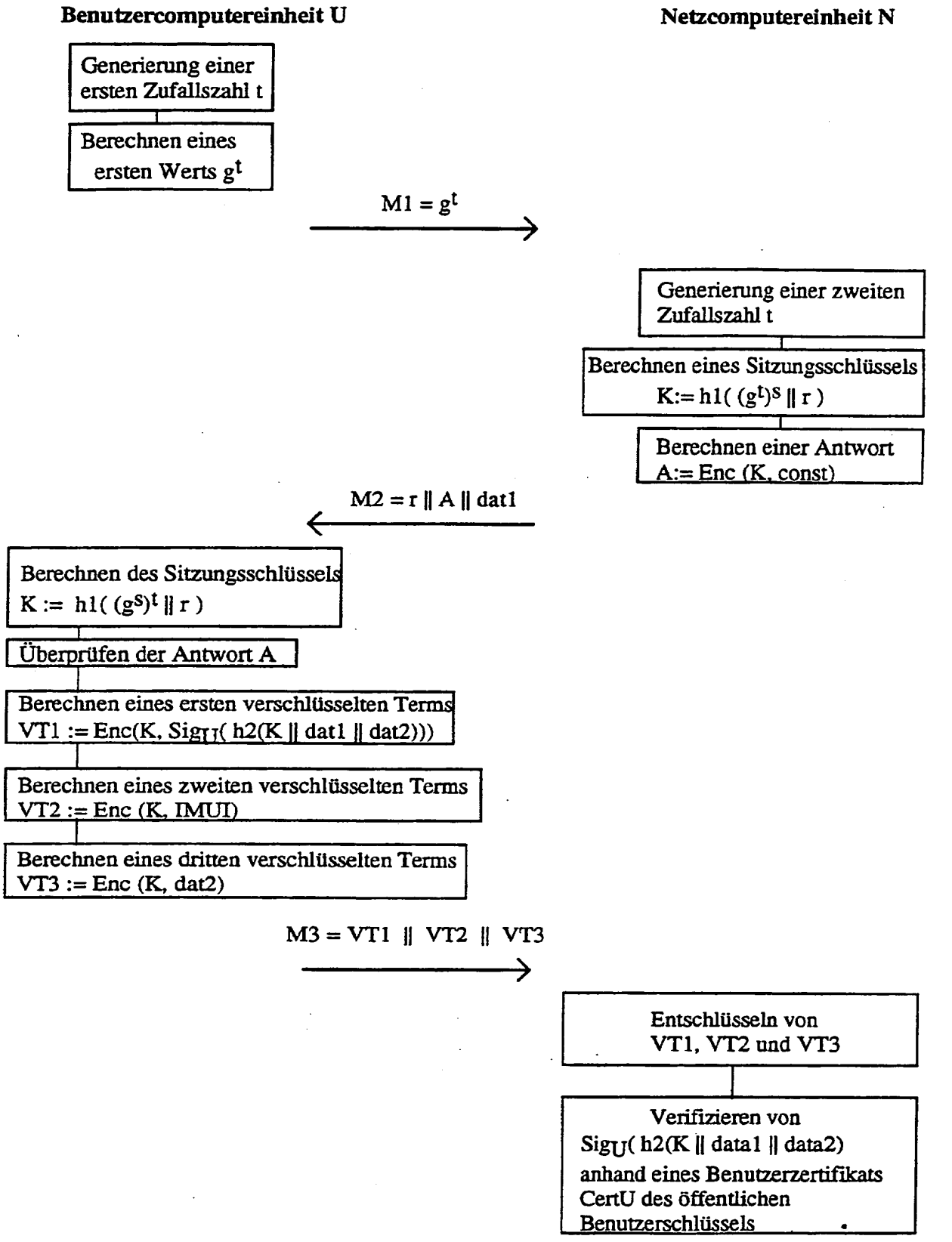
– Leerseite –

Nummer: DE 195 18 546 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 1. August 1996



Figur 1

Nummer: DE 195 18 546 C1
Int. Cl.[6]: H 04 L 9/00
Veröffentlichungstag: 1. August 1996



Figur 2

602 131/259